Beschreibung

Verfahren zur Speicherung von Daten in einem Wahlzugriffspeicher und Verschlüsselungs- und Entschlüsselungsvorrichtung

Die vorliegende Erfindung betrifft ein Verfahren zur Speicherung von Daten in einem Wahlzugriffsspeicher und eine Verschlüsselungs- und Entschlüsselungsvorrichtung.

Zur Gewährleistung von Datensicherheit oder zum Schutz von Urheberrechten ist es bekannt, Daten in Festwertspeichern (ROM), wie beispielsweise EPROM, EEPROM, CD-ROM, DVD-ROM usw., verschlüsselt abzuspeichern. Diese Daten können dabei sowohl Daten ablauffähiger Programme (Programmcodes) als auch Video- oder Audiodaten betreffen. Weiterhin ist es bekannt, Video- oder Audiodaten verschlüsselt von einer Sendeeinrichtung zu einer Empfängereinrichtung zu übertragen.

Eine Nutzung der verschlüsselt abgespeicherten oder verschlüsselt übertragenen Daten soll dadurch nur solchen Nutzern ermöglicht werden, die über eine entsprechende Entschlüsselungseinheit (Decoder) mit einem "passenden" Schlüssel verfügen.

Herkömmliche Verschlüsselungsalgorithmen, wie beispielsweise das DES-Verfahren (DES = Data Encryption Standard) oder das AES-Verfahren (AES = Advanced Encryption Standard) verschlüsseln/kodieren die Daten blockweise, wobei beispielsweise beim DES-Verfahren jeweils 64 Datenbits in einem Block kodiert werden. Da bei diesen Verfahren die Anzahl der in einem Datenblock enthaltenen Datenbits üblicherweise größer ist als die Anzahl der Datenbits eines durch eine Verarbeitungseinheit verarbeitbaren Datenworts, ist es erforderlich, die nach dem Dekodieren eines Datenblockes erhaltenen Datenworte vor ihrer weiteren Verarbeitung durch die Verarbeitungseinheit in einem Wahlzugriffsspeicher (RAM = Random Access Memory) abzulegen.

Solche extern zu der Verarbeitungseinheit angeordneten RAM, stellen insofern ein Sicherheitsrisiko dar, als die Möglichkeit besteht, die entschlüsselten Daten an der Verbindungsstrecke zwischen dem RAM und der Verarbeitungseinheit abzugreifen. Diese Daten, beispielsweise Video- oder Audiodaten, können dann unverschlüsselt abgespeichert und somit einer nicht autorisierten Nutzung zugänglich gemacht werden.

Handelt es sich bei den im RAM abgespeicherten Daten um Daten eines Programmcodes so besteht die Gefahr, dass anhand des unverschlüsselt zugänglichen Programmcodes der Programmablauf durch Unbefugte ermittelt werden kann. Außerdem besteht die Gefahr, dass der das Programm ausführenden Einheit nicht autorisierter Programmcode zugeführt wird, um beispielsweise zusätzliche Funktionalitäten, die durch den autorisierten Programmcode nicht bereitgestellt werden sollen, bereitzustellen.

Ziel der vorliegenden Erfindung ist es ein sicheres Verfahren zur Speicherung von Daten in einem RAM anzugeben, das die genannten Nachteile nicht aufweist und das mit geringem Aufwand realisierbar ist, und eine Vorrichtung zur Verschlüsselung/Entschlüsselung der in einem RAM abzuspeichernden Daten anzugeben.

Diese Ziele werden durch ein Verfahren nach Anspruch 1 und durch eine Vorrichtung nach Anspruch 12 gelöst. Vorteilhafte Ausgestaltungen der Erfindung sind Gegenstand der Unteransprüche.

Das erfindungsgemäße Verfahren zum Speichern von Daten in einem Wahlzugriffsspeicher (RAM), in dem Datenworte mit einer vorgegebenen Anzahl Datenbits abspeicherbar sind, sieht vor, vor der Speicherung eine Verschlüsselung eines jeden Datenwortes vorzunehmen, indem aus jedem Datenwort oder einem aus dem Datenwort abgeleiteten Datenwort durch eineindeutiges Um-

ordnen/Permutieren der einzelnen Datenbits unter Verwendung eines ersten Permutationsschlüssels ein permutiertes Datenwort mit der vorgegebenen Anzahl Datenbits erzeugt wird.

Vorteilhafterweise werden bei diesem Verfahren die einzelnen Datenbits des permutierten Datenwortes vor dem Abspeichern unter Verwendung eines ersten Substitutionsschlüssels substituiert, wobei das durch Permutation und anschließende Substitution erzeugte verschlüsselte Datenwort in dem Speicher abgespeichert wird. In diesem Zusammenhang besteht auch die Möglichkeit, die Datenbits des zu verschlüsselnden Datenwortes vor der Permutation unter Verwendung eines ersten Substitutionsschlüssels zu substituieren und das aus der Substitution und der anschließenden Permutation erhaltene Datenwort als verschlüsseltes Datenwort abzuspeichern.

Die Verschlüsselung der einzelnen Datenworte erfolgt vorzugsweise in demselben Chip, in dem eine die Datenworte verarbeitende Verarbeitungseinheit integriert ist. Die von diesem Chip nach außen an den RAM-Speicher zur Abspeicherung übertragenen Datenworte liegen bei diesem Verfahren verschlüsselt, und damit geschützt gegen Störeinflüsse oder unbefugtes Abgreifen der Daten vor. Die Verschlüsselung erfolgt bei dem Verfahren datenwortweise, so dass - anders als bei einer blockweisen Verschlüsselung - keine zusätzlichen Speicher auf dem Chip für die Verschlüsselung bzw. eine Entschlüsselung erforderlich sind.

Die Permutation bzw. Umordnung der einzelnen Datenbits nach Maßgabe des Permutationsschlüssels stellt ein leistungsfähiges Verschlüsselungsverfahren dar. Bei einem Datenwort der Breite 32 Bit gibt es $32! \approx 2{,}6 \cdot 10^{35}$ verschiedene Permutationsmöglichkeiten. Diese Anzahl der Verschlüsselungsmöglichkeiten erhöht sich bei einem Datenwort der Länge 32 Bit um einen Faktor 2^{32}, wenn neben der Permutation eine Substitution des Eingangsdatenwortes oder des bereits permutierten Datenwortes

unter Verwendung eines Substitutionsschlüssels der Länge 32 Bit vorgenommen wird.

Die Substitution eines zu substituierenden Datenwortes nach Maßgabe des Substitutionsschlüssels erfolgt beispielsweise dadurch, dass jedem Datenbit des Datenwortes ein Schlüsselbit des Substitutionsschlüssels zugeordnet wird, wobei das jeweilige Datenbit abhängig vom Wert des zugeordneten Substitutionsschlüsselbits unverändert oder invertiert auf das aus der Substitution resultierende Datenwort abgebildet wird.

Der Permutationsschlüssel umfasst bei einer Ausführungsform eine der Anzahl der Datenbits des zu permutierenden Datenwortes entsprechende Anzahl eindeutige Teilschlüssel, die jeweils einem Datenbit des aus der Permutation resultierenden permutierten Datenwortes zugeordnet sind. Die einzelnen Teilschlüssel geben an, welches der Datenbits des zu permutierenden Datenwortes auf das jeweilige Datenbit abzubilden ist, dem der Teilschlüssel zugeordnet ist.

Jeder Teilschlüssel des Permutationsschlüssels umfasst dabei eine Anzahl Schlüsselbits, wobei vorzugsweise vorgesehen ist, die Abbildung eines Datenbits des zu permutierenden Datenwortes auf ein Datenbit des permutierten Datenwortes unter Verwendung eines Teilschlüssels stufenweise mit folgenden Verfahrensschritten durchzuführen:

a) Auswählen einer ersten Gruppe von Datenbits aus den Datenbits des zu permutierenden Datenwortes nach Maßgabe eines ersten Schlüsselbits des Teilschlüssels,

b) Auswählen einer zweiten Gruppe von Datenbits aus der anhand der vorherigen Auswahl erhaltenen ersten Gruppe von Datenbits nach Maßgabe eines zweiten Schlüsselbits des Teilschlüssels,

c) Wiederholen des Verfahrensschrittes b) unter Verwendung jeweils eines weiteren Schlüsselbits, um jeweils aus einer durch eine vorherige Auswahl erhaltenen Gruppe eine weitere Gruppe auszuwählen bis die ausgewählte Gruppe nur noch ein Datenbit umfasst, das dem Datenbit des permutierten Datenwortes entspricht.

Ein solches stufenweises Auswahlverfahren zur Abbildung eines Datenbits des zu permutierenden Datenwortes auf ein Datenbit des permutierten Datenwortes bietet den Vorteil, dass zu seiner Realisierung keine Speicherelemente erforderlich sind.

Der Permutationsschlüssel und gegebenenfalls der Substitutionsschlüssel werden vor einem neuen Beschreiben des RAM-Speichers, beispielsweise nach dem Einschalten eines den RAM-Speicher enthaltenden Gerätes, neu erzeugt.

Der Substitutionsschlüssel, der eine der Anzahl der Datenbits entsprechende Anzahl Substitutionsschlüsselbits umfasst, wird dabei erzeugt, indem eine entsprechende Anzahl Bits aus einer durch einen Zufallsgenerator bereitgestellten Sequenz herausgegriffen werden.

Bei der Erzeugung des Permutationsschlüssels ist zu beachten, dass sich die einzelnen Teilschlüssel unterscheiden müssen, um eine eindeutige Zuordnung eines Datenbits des zu permutierenden Datenwortes auf ein Datenbit des permutierten Datenwortes zu gewährleisten. Zur Erzeugung der einzelnen Teilpermutationsschlüssel, die jeweils einer Bitposition des permutierten Datenwortes zugeordnet sind, und die gemeinsam den Permutationsschlüssel ergeben, ist vorgesehen, nacheinander für jede Bitposition des permutierten Datenwortes einen Teilpermutationsschlüssel zu erzeugen und dabei jeweils zu überprüfen, ob der erzeugte Teilpermutationsschlüssel bereits für eine andere Bitposition erzeugt wurde. Wurde dieser Teilpermutationsschlüssel bereits erzeugt, so wird er verworfen und ein neuer Teilpermutationsschlüssel wird für die jeweilige Bitposition zufällig erzeugt. Ist der zufällig

Bitposition zufällig erzeugt. Ist der zufällig erzeugte Teilpermutationsschlüssel noch nicht vorhanden, so wird dieser für die jeweilige Bitposition beibehalten. Dieses Verfahren wiederholt sich, bis jeder Bitposition des permutierten Datenwortes ein Teilpermutationsschlüssel für die Auswahl eines Datenbits des zu permutierenden Datenwortes zugewiesen ist.

Die Entschlüsselung der in dem RAM abgespeicherten Datenworte erfolgt in entsprechender Weise wie das Verschlüsselungsverfahren. Wird bei einem zweistufigen Verfahren mit Permutation und Substitution das zu verschlüsselnde Datenwort zunächst permutiert und dann substituiert, so wird beim Entschlüsseln das verschlüsselte Datenwort zunächst unter Verwendung eines zweiten Substitutionsschlüssels "zurück"-substituiert, um die bei der Verschlüsselung vorgenommene Substitution rückgängig zu machen, und anschließend unter Verwendung eines zweiten Permutationsschlüssels "zurück"-permutiert, um die bei der Verschlüsselung vorgenommene Permutation rückgängig zu machen.

Erfolgt bei der Verschlüsselung des Datenwortes zunächst eine Substitution und dann eine Permutation, so wird bei der Entschlüsselung das verschlüsselte Datenwort zunächst unter Verwendung des zweiten Permutationsschlüssels permutiert und anschließend substituiert, um das ursprüngliche Datenwort zurück zu gewinnen.

Abhängig von der Art der angewendeten Substitution kann der erste Substitutionsschlüssel identisch zu dem zweiten Substitutionsschlüssel gewählt werden, beispielsweise dann, wenn die Substitution darin besteht, nach Maßgabe der Schlüsselbits des Substitutionsschlüssel die einzelnen Datenbits unverändert oder invertiert abzubilden.

Die vorliegende Erfindung wird nachfolgend in Ausführungsbeispielen anhand von Figuren näher erläutert.

Figur 1 zeigt eine Anordnung mit einer Verschlüsselungs- und Entschlüsselungsanordnung, die die in einem Wahlzugriffsspeicher abzuspeichernden Daten verschlüsselt und die aus dem Wahlzugriffsspeicher ausgelesenen Daten entschlüsselt.

Figur 2 zeigt ein Ausführungsbeispiel einer Verschlüsselungs- und Entschlüsselungsanordnung mit einer Verschlüsselungseinheit, einer Entschlüsselungseinheit, einem Schlüsselgenerator und einem Zufallsgenerator.

Figur 3 zeigt ein Ausführungsbeispiel einer Verschlüsselungseinheit, die eine Permutationseinheit und eine Substitutionseinheit umfasst.

Figur 4 veranschaulicht schematisch den Aufbau einer Permutationseinheit, die Auswahleinheiten umfasst.

Figur 5 zeigt ein Ausführungsbeispiel einer Auswahleinheit, die mehrere Auswahlstufen mit Auswahlschaltern umfasst.

Figur 6 veranschaulicht die Funktionsweise einer Auswahleinheit für ein Datenwort der Breite 8 Bit.

Figur 7 zeigt ein schaltungstechnisches Realisierungsbeispiel der in Figur 5 dargestellten Auswahlschalter.

Figur 8 zeigt schematisch ein Ausführungsbeispiel der in Figur 3 dargestellten Substitutionseinheit, die mehrere Substitutionselemente umfasst.

Figur 9 veranschaulicht ein mögliches Realisierungsbeispiel der in Figur 8 dargestellten Substitutionselemente.

Figur 10 veranschaulicht den Aufbau des Permutationsschlüssels aus Teilschlüsseln und Schlüsselbits und den Aufbau des Substitutionsschlüssels.

Figur 11 veranschaulicht den vollständigen Aufbau einer Permutationseinheit für eine Verschlüsselungseinheit gemäß Figur 2 für Datenworte mit 4 Bit.

Figur 12 zeigt die zu der in Figur 11 dargestellten Permutationseinheit korrespondierende Permutationseinheit zur Verwendung in einer Entschlüsselungseinheit gemäß Figur 2.

Figur 13 zeigt schematisch den Aufbau eines in dem Schlüsselgenerator vorhandenen internen Speichers zum Abspeichern eines ersten Permutationsschlüssels für die Verschlüsselung und eines zweiten Permutationsschlüssels für die Entschlüsselung.

In den Figuren bezeichnen, sofern nicht anders angegeben, gleiche Bezugszeichen gleiche Teile und Signale mit gleicher Bedeutung.

Figur 1 zeigt einen Wahlzugriffsspeicher (RAM) 20, der dazu ausgebildet ist, Datenworte der Länge n-Bit abzuspeichern. Der Speicher 20 besitzt einen Eingang 21 zum Einlesen abzuspeichernder Datenworte und einen Ausgang 22 zum Auslesen abgespeicherter Datenworte. Notwendige Steuerleitungen, über welche dem Speicher die Speicheradressen mitgeteilt werden, an welchen die einzelnen Datenworte abgespeichert oder von welchen die einzelnen Datenworte ausgelesen werden sollen, sind in Figur 1 nicht dargestellt.

Die Verarbeitung der in den Speicher 20 eingelesenen Datenworte bzw. der aus dem Speicher ausgelesenen Datenworte erfolgt in einer Datenverarbeitungseinheit 30, beispielsweise einem Prozessor. Abhängig von der Art dieses Prozessors han-

delt es sich bei den in dem Speicher 20 abgelegten Datenworte beispielsweise um Datenworte eines Programmcodes, der durch den Prozessor ausgeführt wird, oder um Datenworte von Video- oder Audiodaten, die über den Prozessor 30 über geeignete Ausgabeeinheiten zur Wahrnehmung gebracht werden.

Die Datenverarbeitungseinheit 30 und der Speicher 20 sind nicht auf einem gemeinsamen Chip integriert, was in Figur 1 durch die gestrichelte Linie zwischen der Datenverarbeitungseinheit 30 und dem Speicher 20 veranschaulicht ist. Um ein "Abhören" oder Stören der Datenkommunikation zwischen der Datenverarbeitungseinheit 30 und dem Speicher 20 zu verhindern, ist zwischen der Datenverarbeitungseinheit 30 und dem Speicher 20 auf dem selben Chip, auf dem die Datenverarbeitungseinheit 30 angeordnet ist, eine Verschlüsselungs- und Entschlüsselungsvorrichtung 10 vorgesehen. Diese Vorrichtung 10 verschlüsselt von der Datenverarbeitungseinheit 30 ausgegebene Datenworte M, um verschlüsselte Datenworte M' zur Verfügung zu stellen, die in dem Speicher 20 wortweise abgelegt werden. In umgekehrter Richtung entschlüsselt die Vorrichtung 10 die in dem Speicher 20 verschlüsselt abgelegten Datenworte M' um das ursprüngliche, durch die Datenverarbeitungseinheit 30 verarbeitbare Datenwort wieder herzustellen. M bezeichnet in der Figur 1 und im Folgenden ein beliebiges unverschlüsseltes Datenwort der Länge n und M' ein beliebiges durch Verschlüsselung eines Datenwortes M entstandenes verschlüsseltes Datenwort der Länge n.

Figur 2 zeigt schematisch den Aufbau einer solchen Verschlüsselungs- und Entschlüsselungsvorrichtung 10. Die dargestellte Vorrichtung umfasst eine Verschlüsselungseinheit 11, die einen Eingang der Breite n-Bit zur Zuführung eines unverschlüsselten Datenwortes M und einen Ausgang 111 zur Ausgabe eines verschlüsselten Datenwortes M' aufweist. Die Verschlüsselung des Datenwortes M erfolgt nach Maßgabe eines ersten Schlüssels C, der durch einen Schlüsselgenerator 13 bereitgestellt wird. Zur Bereitstellung dieses ersten Schlüssels C ist dem

Schlüsselgenerator 13 eine binäre Zufallssequenz RS von einem binären Zufallszahlengenerator 12 zugeführt.

Die Vorrichtung 10 umfasst weiterhin eine Verschlüsselungseinheit 11' mit einem Eingang 110' zur Zuführung eines verschlüsselten Datenwortes M' der Breite n-Bit und mit einem Ausgang 111' zur Bereitstellung des aus dem verschlüsselten Datenwort M' erzeugten entschlüsselten Datenwortes M. Die Entschlüsselung erfolgt nach Maßgabe eines zweiten Schlüssels C', der auf den ersten Schlüssel C abgestimmt ist und der ebenfalls durch den Schlüsselgenerator 13 zur Verfügung gestellt wird.

Die Verschlüsselungseinheit bildet das Datenwort unter Verwendung des ersten Schlüssel C eindeutig auf das verschlüsselte Datenwort M' ab, wobei gilt:

$$M' = E(M,C) \qquad (1),$$

wobei für E die durch die Verschlüsselungseinheit 11 realisierte Verschlüsselungsfunktion steht. Entsprechend gilt:

$$M = D(M',C') \qquad (2).,$$

wobei D für die durch die Entschlüsselungseinheit 11'realisierte Entschlüsselungsfunktion steht.

Figur 3 zeigt schematisch ein Ausführungsbeispiel der Verschlüsselungseinheit 11, die in dem Beispiel eine Permutationseinheit 14 und eine Substitutionseinheit 15 umfasst. Die Permutationseinheit 14 weist Eingänge zur Zuführung der einzelnen Datenbits M[n-1]...M[0] des Datenwortes M und Ausgänge zur Bereitstellung von Datenbits Mp[n-1], Mp[k], Mp[0] eines permutierten Datenwortes Mp auf. Die einzelnen Datenbits Mp[n-1]...Mp[0] des permutierten Datenwortes Mp resultieren aus den Datenbits M[n-1]...M[0] des Datenwortes M durch Permutieren/Umordnen nach Maßgabe eines Permutationsschlüssels

P. Die Permutation erfolgt dabei eineindeutig, das heißt, je ein Datenbit des unverschlüsselten Datenwortes M wird auf ein Datenbit des permutierten Datenwortes Mp abgebildet.

Die Datenbits Mp[n-1]...Mp[0] des permutierten Datenwortes Mp werden in dem Beispiel anschließend durch eine Substitutionseinheit 15 nach Maßgabe eines Substitutionsschlüssels S substituiert, wobei die Substitutionseinheit 15 die Datenbits des verschlüsselten Datenwortes M' bereitstellt. Durch die Substitutionseinheit 15 wird nach Maßgabe des Substitutionsschlüssels S je ein Datenbit des permutierten Datenwortes Mp auf ein Datenbit M'[n-1]...M'[0] des verschlüsselten Datenwortes M' abgebildet.

Der Aufbau und die Funktionsweise der Permutationseinheit 14 werden nachfolgend anhand der Figuren 5 bis 7 erläutert. Anschließend werden der Aufbau und die Funktionsweise der Substitutionseinheit 15 anhand der Figuren 8 und 9 erläutert.

Bezugnehmend auf Figur 4 besitzt die Permutationseinheit 14 eine der Anzahl der Datenbits des zu verschlüsselnden Datenwortes M entsprechende Anzahl Auswahleinheiten 14_n-1...14_0, wobei jeder dieser Auswahleinheiten alle Datenbits M[n-1]...M[0] des zu verschlüsselnden Datenwortes M zugeführt sind und wobei die einzelnen Auswahleinheiten 14_n-1...14_0 jeweils ein Datenbit Mp[n-1]...Mp[0] des permutierten Datenwortes Mp zur Verfügung stellen. Die Abbildung eines der Datenbits des unverschlüsselten Datenwortes M auf eines der Datenbits des permutierten Datenwortes Mp erfolgt in den Auswahleinheiten 14_n-1...14_0 nach Maßgabe von Teilpermutationsschlüsseln P[n-1], P[k], P[0]. Diese Teilpermutationsschlüssel unterscheiden sich jeweils, um jedes der Datenbits des Eingangsdatenwortes M genau einmal auf ein Datenbit des permutierten Datenwortes Mp abzubilden, Die Teilpermutationsschlüssel ergeben gemeinsam den Permutationsschlüssel, wobei gilt: P = (P[n-1], ... P[0]).

Die einzelnen Auswahleinheiten 14_n-1...14_0 sind identisch aufgebaut, wobei der Aufbau einer beliebigen dieser Auswahleinheiten, im vorliegenden Fall der Auswahleinheit 14_k nachfolgend anhand von Figur 5 erläutert wird.

Diese Auswahleinheit 14_k stellt das Datenbit Mp[k] aus den Datenbits M[n-1]...M[0] des Datenwortes M nach Maßgabe des Teilpermutationsschlüssels P[k] zur Verfügung. Dieser Teilpermutationsschlüssel umfasst m Schlüsselbits P[k,m-1]...P[k,0].

Die Auswahleinheit 14_k umfasst mehrere Auswahlstufen 141_0...141_m-1. Einer ersten Auswahlstufe 141_0 sind dabei alle Datenbits des Eingangsdatenwortes M zugeführt. Diese erste Auswahlstufe 141_0 wählt nach Maßgabe eines ersten Schlüsselbits P[k,0] des Teilpermutationsschlüssels P[k] eine erste Gruppe von Datenbits aus, die einer zweiten Auswahlstufe 141_1 zugeführt sind. Die zweite Auswahlstufe 141_1 bildet aus dieser ersten Gruppe nach Maßgabe eines zweiten Schlüsselbits P[k,1] eine zweite Gruppe, die der dritten Auswahleinheit 141_2 zugeführt ist.

In dem dargestellten Beispiel erfolgt von Auswahlstufe zu Auswahlstufe eine Reduktion der in den jeweiligen Gruppen vorhandenen Datenbits um einen Faktor 2, so dass nach $m = \log_2(n)$ Auswahlstufen nur noch ein Datenbit vorhanden ist, das dem Datenbit Mp[k] des permutierten Datenwortes Mp entspricht. In dem Beispiel, in dem $n = 32 = 2^5$ gilt, sind somit $m = 5$ Auswahlstufen vorhanden.

Jede der Auswahlstufen umfasst in dem Beispiel eine Anzahl von Auswahlschaltern 142, denen jeweils zwei Datenbits einer Datengruppe zugeführt sind, und die jeweils nach Maßgabe eines Permutationsschlüsselbits eines der beiden Datenbits auswählen und an die nächste Auswahlstufe weitergeben.

Die Zuführung der einzelnen Datenbits zu den Auswahlschaltern der jeweiligen Auswahlstufe erfolgt derart, dass einem Auswahlschalter jeweils zwei Datenbits zugeführt sind, die bezogen auf die Gruppe, aus denen die jeweilige Auswahlstufe eine Auswahl trifft, aufeinanderfolgende Bitpositionen besitzen. In dem Beispiel gemäß Figur 5 wird dabei das jeweils höherwertige Bit einem ersten Eingang IN1 und das jeweils niederwertigere Bit einem zweiten Eingang IN2 des jeweiligen Auswahlschalters 142 zugeführt sind. Bei einem Schlüsselbit "1" wird in dem dargestellten Beispiel das am Eingang IN1 anliegende Bit, also das höherwertige Bit an den Ausgang OUT1 und damit an die nächste Auswahlstufe weitergegeben.

Die Funktionsweise der in Figur 5 dargestellten Auswahleinheit wird nachfolgend anhand eines 8 Bit breiten Datenwortes M in Figur 6 erläutert. Von diesen 8 Datenbits M[7]...M[0] wird eines ausgewählt, um das Datenbit Mp[k] des permutierten Datenwortes zu bilden. Das erste Schlüsselbit P[k,0] des Teilschlüssels P[k] beträgt 1, so dass von jeweils zwei in ihrer Wertigkeit aufeinanderfolgenden Datenbits das jeweils höherwertige ausgewählt wird, woraus eine erste Gruppe mit den Datenbits M[7], M[5], M[3], M[1] resultiert. Von jeweils zwei bezüglich ihrer Wertigkeit aufeinanderfolgenden Datenbits, also den Datenbits M[7], M[5] und M[3], M[1] wird nach Maßgabe des zweiten Schlüsselbits P[k,1] je ein Datenbit ausgewählt. Dieses Schlüsselbit ist in dem Beispiel "0", so dass jeweils das niederwertigere der beiden Datenbits, also die Datenbits M[5], M[1] ausgewählt werden. Aus dieser resultierenden weiteren Gruppe von Datenbits wird nach Maßgabe des dritten Schlüsselbits P[k,2] eines, im vorliegenden Fall das höherwertigere, also das Datenbit M[5] ausgewählt, um das Datenbit Mp[k] des permutierten Datenwortes zu bilden.

Ordnet man die Datenbits in jeder der Auswahlgruppen abhängig von Ihrer Wertigkeit und wählt man von zwei in ihrer Wertigkeit benachbarten Datenbits bei einem Schlüsselbit "1" jeweils das höherwertigere und bei einem Schlüsselbit "0" je-

weils das niederwertigere dieser beiden Datenbits aus, so entspricht der Wert der Bit-Position des ausgewählten Datenbits, im vorliegenden Fall des Datenbits M[5], dem dezimalen Äquivalent des Teilsschlüssels P[k], wie nachfolgend erläutert ist:

Betrachtet man den Teilschlüssel P[k] als binäre Zahlenfolge, dessen signifikantestes Bit (MSB) durch das Schlüsselbit P[k,m-1] der letzten Auswahlstufe und dessen am wenigsten signifikante Bit (LSB) durch das Schlüsselbit P[k,0] der ersten Auswahlstufe gebildet wird, so entspricht das dezimale Äquivalent dieser Binärfolge, im vorliegenden Fall $101_2 = 5_{10}$ der Bitposition des aus dem Datenwort M ausgewählten Datenbits M[5].

Ein schaltungstechnisches Realisierungsbeispiel eines der Auswahlschalter 142 ist in Figur 7 dargestellt. Zur Realisierung der erläuterten Auswahlfunktion umfasst der Auswahlschalter zwei UND-Gatter AND1, AND2, deren Ausgänge einem ODER-Gatter OR1 zugeführt sind, wobei der Ausgang dieses ODER-Gatters den Ausgang OUT1 des Auswahlschalters bildet. Je einer der Eingänge IN1, IN2 zur Zuführung der Datenbits ist einem der UND-Gatter AND1, AND2 zugeführt. Der andere Eingang des UND-Gatters AND1 ist an den dritten Eingang IN3 zur Zuführung eines Schlüsselbits gekoppelt, wobei dem anderen Eingang des UND-Gatters AND2 dieses Schlüsselbit invertiert über einen Inverter INV1 zugeführt ist. Bei Anlegen einer logischen "1" am dritten Eingang IN3 wird somit das am ersten Eingang IN1 anliegende Datenbit über das erste UND-Gatterbit AND1 und das ODER-Gatter OR1 an den Ausgang OUT1 weitergegeben. Bei einer logischen "0" am dritten Eingang IN3 wird entsprechend das Datenbit am zweiten Eingang IN2 über das zweite UND-Gatter AND2 und das ODER-Gatter OR1 an den Ausgang OUT1 weitergegeben.

Bezugnehmend auf Figur 8 umfasst die Substitutionseinheit 15 eine der Anzahl der Datenbits entsprechende Anzahl Substitu-

tionselemente 15_n-1...15_0, denen jeweils ein Datenbit des zu substituierenden Datenwortes, in dem Beispiel gemäß Figur 3 des permutierten Datenwortes Mp, zugeführt sind. Der Schlüssel S, nach dessen Maßgabe die Substitution erfolgt, umfasst n Schlüsselbits S[n-1]...S[0], wobei jedem der Substitutionselemente eines dieser Schlüsselbits S[n-1]...S[0] zugeführt ist. Die Substitutionselemente 15_n-1...15_0 sind dazu ausgebildet, nach Maßgabe des jeweiligen Substitutionsschlüsselbits S[n-1]...S[0] das dem jeweiligen Substitutionselement 15_n-1...15_0 zugeführte Datenbit Mp[n-1]...Mp[0] unverändert oder invertiert auszugeben.

Ein schaltungstechnisches Realisierungsbeispiel eines solchen Substitutionselements ist in Figur 9 dargestellt. Das Substitutionselement 15_k umfasst ein erstes und zweites UND-Gatter AND3, AND4 und ein den UND-Gattern AND3, AND4 nachgeschaltetes ODER-Gatter OR2 an dessen Ausgang das substituierte Datenbit zur Verfügung steht. Das zu substituierende Datenbit wird dem Substitutionselement über einen ersten Eingang IN4 zugeführt, wobei dieses Datenbit über einen ersten Inverter INV2 dem ersten UND-Gatter AND3 invertiert und dem zweiten UND-Gatter AN4 unverändert zugeführt ist. Das an einem zweiten Eingang IN5 des Substitutionselements anliegende jeweilige Substitutionsschlüsselbit wird dem ersten Gatter AND3 unverändert und dem zweiten UND-Gatter AND4 invertiert mittels eines zweiten Inverters INV3 zugeführt. Diese Anordnung gewährleistet, dass bei einem Substitutionsschlüsselbit "1" das am ersten Eingang IN4 anliegende Datenbit invertiert und bei einem Substitutionsschlüsselbit "0" unverändert am Ausgang OUT2 zur Verfügung gestellt wird.

In dem Ausführungsbeispiel gemäß Figur 3 wird das verschlüsselte Datenwort M' aus dem unverschlüsselten Datenwort M durch Permutation und anschließende Substitution des aus der Permutation resultierenden permutierten Datenwortes Mp erzeugt. Selbstverständlich besteht auch die Möglichkeit, das Datenwort M zunächst unter Verwendung des Substitutions-

schlüssels M zu substituieren und das daraus resultierende substituierte Datenwort anschließend unter Verwendung des Permutationsschlüssels P zu permutieren, um zu dem verschlüsselten Datenwort M' zu gelangen.

Maßgeblich für die Leistungsfähigkeit eines Verschlüsselungssystems ist die Anzahl möglicher unterschiedlicher Schlüssel. Der Schlüssel C zur Verschlüsselung eines Datenwortes M setzt sich in dem erläuterten Beispiel aus einem Permutationsschlüssel P und einem Substitutionsschlüssel S zusammen. Der Permutationsschlüssel P umfasst eine der Anzahl der Datenbits entsprechende Anzahl Teilschlüssel für deren Länge $m=\log_2(n)$ gilt. Bezugnehmend auf Figur 10 kann der Permutationsschlüssel als Vektor mit n Teilschlüsseln P[n-1]...P[0] oder als n x m-Matrix der einzelnen Teilschlüsselbits P[n-1,m-1]...P[0,0] betrachtet werden. Für Datenworte der Länge n=32 umfasst der Permutationsschlüssel 32 jeweils verschiedene Teilschlüssel P[n-1]...P[0] woraus 32! unterschiedliche Schlüsselkombinationen resultieren. Berücksichtigt man dass für den Substitutionsschlüssel S 2^n Möglichkeiten zur Verfügung stehen, so ergibt sich für die Anzahl N der möglichen Schlüssel C für zu verschlüsselnde Datenworte der Länge n=32: $N = (32!)\cdot 2^{32}$.

Der Substitutionsschlüssel S für die Verschlüsselung und die Entschlüsselung kann auf einfache Weise als Teil einer binären Zufallssequenz erzeugt werden.

Ein Verfahren zur Erzeugung des Permutationsschlüssels wird nachfolgend für ein Datenwort der Länge n=4 Bit anhand der Figuren 11 bis 13 erläutert.

Figur 11 zeigt zunächst eine erste Permutationseinheit 14 zur Erzeugung eines permutierten Datenwortes Mp aus einem Datenwort M mit n=4 Auswahleinheiten 14_3, 14_2, 14_1, 14_0, die jeweils 2-stufig ($m=\log_2 4=2$) ausgebildet sind.

Figur 12 zeigt eine zu der Permutationseinheit 14 gemäß Figur 11 korrespondierende zweite Permutationseinheit, die zum Rückgängigmachen der durch die erste Permutationseinheit 14 vorgenommenen Permutation beim Entschlüsseln des Datenwortes in der Entschlüsselungseinheit (11 in Figur 3) dient. Diese zweite Permutationseinheit 14' ist identisch zu der ersten Permutationseinheit 14 aufgebaut und umfasst vier Auswahleinheiten 14'_3, 14'_2, 14'_1, 14'_0. Jede dieser Auswahleinheiten 14'_3 ... 14'_0 dient dazu, eines der Datenbits Mp[3]...Mp[0] des permutierten Datenwortes Mp auf eines der Datenbits M[3]...M[0] des ursprünglichen Datenwortes M zurück abzubilden. Diese Auswahl eines der Datenbits in den einzelnen Auswahleinheiten 14'_3...14'_0 erfolgt jeweils nach Maßgabe von Teilschlüsseln P'[3]... P'[0] eines zweiten Permutationsschlüssels P', wobei in dem dargestellten Beispiel gilt: P' =(P'[3], P'[2], P'[1], P'[0]), wobei die einzelnen Teilschlüssel P'[3]...P'[0] jeweils zwei Teilschlüsselbits P'[3,1]...P'[0,0] umfassen.

Die Erzeugung der Teilschlüssel P[3]... P[0] des ersten Permutationsschlüssels P sowie der zugehörigen Teilschlüssel P'[3]...P'[0] des zweiten Permutationsschlüssels P' wird nachfolgend anhand von Figur 13 erläutert.

Zur Erzeugung des ersten und zweiten Permutationsschlüssels P, P' umfasst der Schlüsselgenerator (13 in Figur 2) einen ersten und einen zweiten Schlüsselspeicher 131, 131' sowie ein Zuordnungsregister 132. Die Schlüsselspeicher 131, 131' sind dazu ausgebildet, jeweils n Teilschlüssel der Schlüsselbreite $m=\log_2(n)$ zu speichern. Für n=4 sind in jedem Schlüsselspeicher vier Teilschlüssel der Länge 2 abspeicherbar. Die Zuordnung der in dem ersten Schlüsselspeicher 131 abgespeicherten Teilschlüssel zu den Auswahleinheiten 14_3...14_0 und damit zu den einzelnen Datenbits des permutierten Datenwortes Mp erfolgt über die Adresse des Schlüsselspeichers 131, der zeilenweise adressierbar ist und der in dem Beispiel n=4 Zeilen umfasst. Die Speicheradresse eines Teilschlüssels in die-

sem ersten Speicher 131 entspricht dabei der Bitposition des Datenbits des permutierten Datenwortes, der der jeweilige Schlüssel zugeordnet ist. Ein Teilschlüssel P[k] an der Speicheradresse k des Schlüsselspeichers 131 ist damit dem k-ten Datenbit Mp[k] des permutierten Datenwortes Mp zugeordnet, wobei k eine der möglichen Zeilenadressen 0...n-1 des Speichers repräsentiert.

Die Zuordnung der Teilschlüssel P'[3]...P'[0] des zweiten Teilschlüssels P' zu den Auswahleinheiten 14'_3 ... 14'_0 bzw. den Datenbits M[3]...M[0] des ursprünglichen Datenwortes erfolgt in entsprechender Weise. Das heißt, der an der Speicherposition k des zweiten Schlüsselspeichers 131' abgespeicherte Teilschlüssel P'[k] ist der Auswahleinheit 14'_k zugeordnet und bestimmt, welches der Datenbits des permutierten Datenwortes Mp auf das Datenbit M[k] an der k-ten Position des Datenwortes M abgebildet werden soll.

Die Erzeugung der Teilschlüssel P[3]...P[0] des ersten Permutationsschlüssels und der zweiten Teilschlüssel P'[3]...P'[0] erfolgt aufeinander abgestimmt in der im folgenden erläuterten Weise.

Die Teilschlüssel des ersten Permutationsschlüssels P werden aufeinanderfolgend als zufällige Binärsequenzen der Länge m=2 unter Verwendung des in Figur 2 dargestellten Funktionsgenerators 12 erzeugt. Wie erläutert müssen sich die einzelnen Teilschlüssel voneinander unterscheiden, um eine eindeutige Zuordnung der Datenbits des zu permutierenden Datenwortes M auf die Datenbits des permutierten Datenwortes Mp zu erreichen. In dem anhand der Figuren 11 und 12 erläuterten Beispiel gibt es n=4 unterschiedliche Teilschlüssel, die den vier Auswahleinheiten beliebig zugeordnet werden können.

Jedem der im vorliegenden Fall möglichen unterschiedlichen Teilschlüssel "11", "10", "01", "00" ist eine Speicherposition des Zuordnungsregisters 132 zugeordnet, wobei in dem Zu-

ordnungsregister an der jeweiligen Speicherposition ein vorgegebener Wert eingetragen wird, wenn der zugeordnete Teilschlüssel bereits an einer Speicherposition des Speichers 131, und damit für eine der Auswahleinheiten 14_3...14_0, bereits erzeugt wurde, um ein erneutes Erzeugen desselben Schlüssels an einer anderen Speicheradresse und damit für eine andere Auswahleinheit 14_3...14_0 zu vermeiden.

Die Zuordnung eines bestimmten der möglichen Teilschlüssel zu einer Speicheradresse des Zuordnungsregisters 132 erfolgt in dem Beispiel durch unmittelbares Abbilden des durch den Teilschlüssel repräsentierten Wert auf die Adresse der Speicherposition des Abbildungsspeichers 132. So ist einem Teilschlüssel "10" beispielsweise die Speicherposition 10_2=2 des Zuordnungsspeichers 132 zugeordnet. Gilt für einen Teilschlüssel allgemein $P[k]=w_{n-1} \ldots w_0$, so gilt für die diesem Teilschlüssel zugeordnete Adresse W des Abbildungsspeichers:

$$W = \sum_{i=0}^{i=n-1} w_i 2^i$$

Für die Erzeugung des Permutationsschlüssels werden aufeinanderfolgend für die einzelnen Speicheradressen des ersten Permutationsschlüsselspeichers 131 jeweilige Teilschlüssel zufällig erzeugt, wobei nach Erzeugung eines jeweiligen Teilschlüssels anhand der Überprüfung des Zuordnungsregisters ermittelt wird, ob ein solcher Teilschlüssel bereits erzeugt wurde. Wurde ein solcher Teilschlüssel bereits erzeugt, so wird der Teilschlüssel verworfen und ein neuer Teilschlüssel wird zufällig generiert. Dieser Vorgang wird solange wiederholt, bis Teilschlüssel für alle Speicherpositionen, und damit für alle Auswahleinheiten der Permutationseinheit 14 erzeugt wurden.

Wird einer der möglichen Teilschlüssel zum ersten Mal erzeugt, so wird an der diesem Schlüssel zugeordneten Speicheradresse des Zuordnungsspeichers 132 ein bestimmter Wert, bei-

spielsweise eine "1" eingetragen. Wird dieser Teilschlüssel zufällig für eine andere Speicherposition des Speichers 131 nochmals erzeugt, wird dies anhand des eingetragenen Wertes in dem Zuordnungsspeicher 132 erkannt, und der Teilschlüssel wird für diese andere Speicherposition verworfen.

Wie bereits erläutert, entspricht der binäre Wert eines Teilschlüssels P[3]...P[0], der einer Auswahleinheit 14_3...14_0 bzw. einem Datenbit Mp[3]...Mp[0] des permutierten Datenwortes Mp zugeordnet ist, der Datenposition des durch die jeweilige Auswahleinheit ausgewählten Datenbits M[3]...M[0] des Eingangswortes M. Entsprechend geben die Teilschlüssel P'[n-1]...P'[0] des zweiten Permutationsschlüssels P' jeweils an, welches der Datenbits des permutierten Datenwortes Mp auf das Datenbit M[3]...M[0] abgebildet werden soll, dem der jeweilige Teilschlüssel zugeordnet ist.

Gilt allgemein, dass ein dem k-ten Datenbit Mp[k] des permutierten Datenwortes Mp zugeordneter Teilschlüssel P[k] das i-te Datenbit M[i] des zu permutierenden Datenwortes auf dieses Datenbit des permutierten Datenwortes Mp abbildet, so muss umgekehrt, der dem i-ten Datenbit zugeordnete Teilschlüssel P'[i] das k-te Datenbit des permutierten Datenwortes Mp auf dieses Datenbit abbilden.

Der zweite Schlüsselspeicher 131' ist entsprechend des ersten Schlüsselspeichers 131 organisiert, das heißt die Adressen, an denen die einzelnen Teilschlüssel P'[n-1]...P'[0] abgespeichert sind, entsprechen den Bitpositionen der Datenbits M[n-1]...M[0], denen die einzelnen Teilschlüssel zugeordnet sind.

Um nun zu einem zufällig erzeugten, dem k-ten Datenbit des permutierten Datenwortes Mp zugeordneten Teilschlüssel P[k] des ersten Permutationsschlüssels P einen passenden Teilschlüssel des zweiten Permutationsschlüssels P' zu erzeugen, wird der Adresswert k des ersten Teilschlüssels P[k] an der

Adresse in dem zweiten Schlüsselspeicher 131' eingetragen, deren Wert dem durch den ersten Schlüssel repräsentieren Binärwert i entspricht. Für P[k]=i gilt also: P'[i]=k

Die Erzeugung des ersten und zweiten Permutationsschlüssels lässt sich anhand des folgenden Algorithmus beschreiben:

```
Zeile 1:   FOR k = (n-1) DOWNTO 0
Zeile 2:     Hole Zufallszahl vom Generator und berechne i
Zeile 3:     Prüfe, ob MapReg (i) = 1 gilt, falls ja, gehe zu
             Zeile 2
Zeile 4:     Setze MapReg(i)  = 1
Zeile 5:     Setze o_store(k) = i
Zeile 6:     Setze i_store(i) = k
Zeile 4:   NEXT k.
```

MapReg(i) steht dabei für den Wert an der Adresse k des Zuordnungsregisters. o_store(k) steht für den Wert an der Adresse k des ersten Speichers, und i_store(i) steht für den Wert an der Adresse i des zweiten Speichers 131'.

Wie bereits erläutert wird die bei der Verschlüsselung und entsprechend bei der Entschlüsselung vorgenommene Permutation durch eine Substitution nach Maßgabe eines Substitutionsschlüssels ergänzt. Diese Substitution kann beim Verschlüsseln sowohl vor der Permutation als auch nach der Permutation erfolgen, wobei bei der Entschlüsselung in umgekehrter Reihenfolge vorgegangen wird. Erfolgt beim Verschlüsseln die Substitution nach der Permutation, so erfolgt beim Entschlüsseln die erneute Substitution vor der Permutation. Bei der bereits erläuterten Substitution, bei der nach Maßgabe der Substitutionsschlüsselbits des jeweils zugeordnete Datenbit invertiert oder unverändert weitergegeben wird, wird beim Entschlüsseln derselbe Substitutionsschlüssel wie beim Verschlüsseln verwendet.

Bezugszeichenliste

AND1-AND4	UND-Gatter
C,C'	Schlüssel
IN1-IN5	Eingänge
INV1, INV2	Inverter
M	Datenwort
M[n-1]... M[0]	Datenbits
M'[n-1]...M'[0]	Datenbits eines verschlüsselten Datenwortes
Mp[n-1]...Mp[0]	Datenbits eines permutierten Datenwortes
OR1, OR2	ODER-Gatter
OUT1, OUT2	Ausgänge
P	Permutationsschlüssel
P[n-1]...P[0]	Teilschlüssel eines Permutationsschlüssels
S	Substitutionsschlüssel
	tes
10	Verschlüsselungs- und Entschlüsselungseinheit
11	Verschlüsselungseinheit
11'	Entschlüsselungseinheit
13	Schlüsselgenerator
14	Permutationseinheit
14_n-1...14_0	Auswahleinheit
15	Substitutionseinheit
15_n-1...15_0	Substitutionseinheiten
20	Wahlzugriffsspeicher, RAM
20	Zufallsgenerator
21	Eingang des RAM
22	Ausgang des RAM
30	Datenverarbeitungseinheit
110	Eingang der Verschlüsselungseinheit
110'	Eingang der Entschlüsselungseinheit
111	Ausgang der Verschlüsselungseinheit
111'	Ausgang der Entschlüsselungseinheit

112	Schlüsseleingang der Verschlüsselungseinheit
112'	Schlüsseleingang der Entschlüsselungseinheit
131	erster Permutationsschlüsselspeicher
131'	zweiter Permutationsschlüsselspeicher
132	Auswahlregister
141_n-1... 141_0	Auswahlstufen
142	Auswahlschalter

Patentansprüche

1. Verfahren zum Speichern von Daten in einem Wahlzugriffsspeicher, in dem Datenworte, die jeweils eine vorgegebene Anzahl Datenbits umfassen, abspeicherbar sind, dadurch gekennzeichnet, dass vor der Speicherung eine Verschlüsselung eines jeden Datenwortes (M) erfolgt, indem aus jedem Datenwort (M) oder einem aus dem Datenwort (M) abgeleiteten Datenwort durch eineindeutiges Permutieren der einzelnen Datenbits (M[n-1]-M[0]) unter Verwendung eines ersten Permutationsschlüssels (P), ein permutiertes Datenwort (Mp) mit der vorgegebenen Anzahl Datenbits erzeugt wird.

2. Verfahren nach Anspruch 1, bei dem die einzelnen Datenbits (M[n-1]-M[0]) des permutierten Datenwortes (Mp) vor dem Abspeichern unter Verwendung eines ersten Substitutionsschlüssels substituiert werden, um das verschlüsselte Datenwort (M') zur Verfügung zu stellen.

3. Verfahren nach Anspruch 1, bei dem die einzelnen Datenbits des Datenwortes (M) vor dem Umordnen unter Verwendung eines ersten Substitutionsschlüssels (S) substituiert werden, um ein substituiertes Datenwort zur Verfügung zu stellen.

4. Verfahren nach einem der vorangehenden Ansprüche, bei dem der Permutationsschlüssel (P) eine der Anzahl n der Datenbits entsprechende Anzahl eindeutige Teilschlüssel (P[n-1]-P[0]) aufweist, die jeweils einem Datenbit (Mp[n-1]-Mp[0]) des permutierten Datenwortes (Mp) zugeordnet sind, und die jeweils das auf dieses Datenbit (Mp[n-1]-Mp[0]) abzubildende Datenbit (M[n-1]-M[0]) des zu permutierenden Datenwortes (M) angeben, wobei jeder Teilschlüssel (P[n-1]-P[0]) eine Anzahl Schlüsselbits (P[n-1,m-1]-P[n-1,0], P[k,m-1]-P[k,0], P[0,m-1]-P[0,0]) umfasst.

5. Verfahren nach Anspruch 4, bei dem die Abbildung eines Datenbits (M[n-1]-M[0]) des zu permutierenden Datenwortes (M) auf ein Datenbit (Mp[k]) des permutierten Datenwortes unter Verwendung eines Teilschlüssels (P[k]) stufenweise mit folgenden Verfahrensschritten erfolgt:

a) Auswählen einer ersten Gruppe von Datenbits des zu permutierenden Datenwortes (Mp) nach Maßgabe eines ersten Schlüsselbits (P[k,0]) des Teilschlüssels (P[k]),

b) Auswählen einer zweiten Gruppe von Datenbits aus der ersten Gruppe von Datenbits nach Maßgabe eines zweiten Schlüsselbits (P[k,1]) des Teilschlüssels (P[k]),

c) Wiederholen des Verfahrensschrittes b) unter Verwendung jeweils eines weiteren Schlüsselbits (P[k,2]...P[k,m-1]) bis die ausgewählte Gruppe nur noch ein Datenbit umfasst, das dem Datenbit (Mp[k]) des permutierten Datenwortes (Mp) entspricht.

6. Verfahren nach Anspruch 5, bei dem die Anzahl der in einer Gruppe von Datenbits enthaltenen Datenbits von Stufe zu Stufe um einen Faktor 2 reduziert wird.

7. Verfahren nach einem der vorangehenden Ansprüche, bei dem der erste Substitutionsschlüssel (S) eine der Anzahl der Datenbits des zu substituierenden Datenwortes (Mp) entsprechende Anzahl Schlüsselbits (S[n-1]...S[0]) aufweist, wobei jedes Datenbit des zu substituierenden Datenwortes (Mp) nach Maßgabe eines dieser Schlüsselbits (S[n-1]...S[0]) unverändert oder invertiert auf ein Datenbit (M'[n-1]...M'[0]) des substituierten Datenwortes (M') abgebildet wird.

8. Verfahren nach einem der vorangehenden Ansprüche, bei dem der Permutationsschlüssel (P) und der Substitutionsschlüssel (S) vor einem neuen Beschreiben des Speichers nach einem Löschen neu erzeugt werden.

9. Verfahren nach einem der vorangehenden Ansprüche, das zur Erzeugung eines Permutationsschlüssels (P) folgende Verfahrensschritte umfasst:

a) zufälliges Erzeugen eines Teilpermutationsschlüssels und Zuordnen des Teilschlüssels einer Bitposition des permutierten Datenwortes,

b) Überprüfen, ob der erzeugte Teilpermutationsschlüssel bereits für eine andere Bitposition des permutierten Datenwortes erzeugt wurde, und Beibehalten des erzeugten Teilpermutationsschlüssels, wenn er noch nicht erzeugt wurde, und Verwerfen des erzeugten Teilpermutationsschlüssels, wenn er bereits erzeugt wurde.

c) Durchführen der Verfahrensschritte a) und b) bis für jede Bitposition des permutierten Datenwortes (Mp) ein Teilschlüssel erzeugt ist.

10. Verfahren nach einem der vorangehenden Ansprüche, bei dem ein aus einem Datenwort (M) unter Verwendung des ersten Schlüssels erzeugtes Datenwort (M') nach dem Auslesen aus dem Speicher unter Verwendung eines zweiten Permutationsschlüssel (P'), der auf den ersten Permutationsschlüssel (P) abgestimmt ist, permutiert wird, um das Datenwort zu erzeugen.

11. Vorrichtung zur Verschlüsselung/Entschlüsselung eines Datenbits (M[n-1], M[k], M[0]) umfassenden Datenwortes (M), die eine Permutationseinheit (14) mit folgenden Merkmale aufweist:

- Dateneingänge zur Zuführung der Datenbits (M[n-1], M[k], M[0]) des zu permutierenden Datenwortes (M),

- Ausgänge zur Bereitstellung der Datenbits (Mp[n-1], Mp[k], Mp[0]) eines permutierten Datenwortes (Mp) der vorgegebenen Länge (n),

- Permutationsschlüsseleingänge zur Zuführung eines Permutationsschlüssels (P), der eine der Anzahl der Datenbits entsprechende Anzahl (n) Teilschlüssel (P[n-1]... P[0]) umfasst,

- eine der Anzahl der Datenbits entsprechende Anzahl Auswahleinheiten (14_n-1, 14_k, 14_0), denen jeweils ein Teilschlüssel zugeordnet ist und die jeweils ein Datenbit (Mp[n-1], Mp[k], Mp[0]) des permutierten Datenwortes (Mp) nach Maßgabe je eines der Teilschlüssel (P[n-1]... P[0]) aus den Datenbits des zu permutierenden Datenwortes (M) bereitstellen.

12. Vorrichtung nach Anspruch 11, bei der jede Auswahleinheit (14_k) eine der Anzahl von Permutationsschlüsselbits der Teilschlüssel entsprechende Anzahl aufeinanderfolgend angeordneter Auswahlstufen (141_n-1, 141_k, 141_0) aufweist, wobei eine erste Auswahlstufe (141_0) dazu ausgebildet ist, nach Maßgabe eines ersten Schlüsselbits (P[k,0]) eine erste Gruppe von Datenbits aus dem zu permutierenden Datenwort (M) auszuwählen und bereitzustellen, und wobei nachfolgende Auswahlstufen (141_1, 141_2, 141_m-1) dazu ausgebildet sind, jeweils nach Maßgabe eines Schlüsselbits (P[k,1], P[k,2], P[k,m-1]) aus der von der jeweils vorherigen Auswahlstufe bereitgestellten Gruppe von Datenbits eine Untergruppe auszuwählen.

13. Vorrichtung nach Anspruch 11 oder 12, bei der der Permutationseinheit (14) eine Substitutionseinheit vorgeschaltet oder nachgeschaltet ist, die nach Maßgabe eines Substitutionsschlüssels (S) Datenbits (Mp[n-1], Mp[k], Mp[0]) eines zu substituierenden Datenwortes (Mp) substituiert.

FIG 1

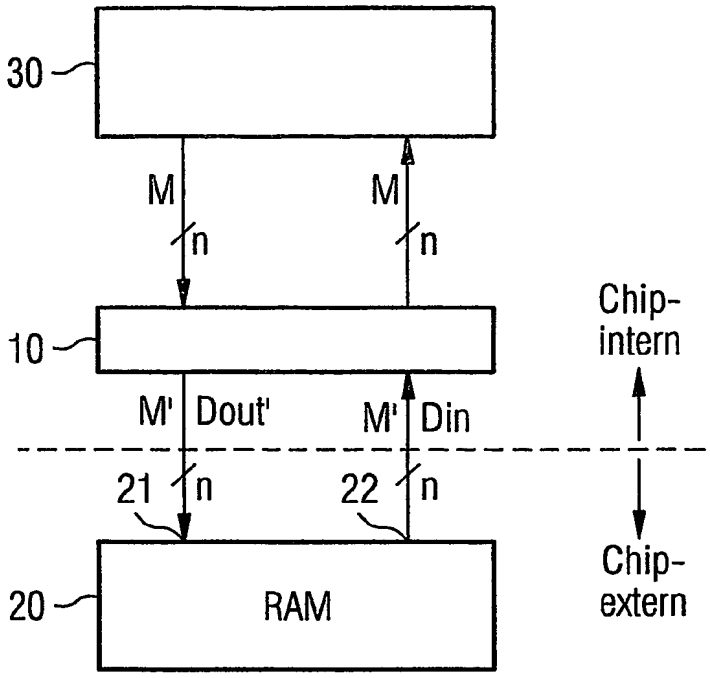

30
M
n
M
n
10
Chip-
intern
M'
Dout'
M'
Din
21
n
22
n
Chip-
extern
20
RAM

FIG 2

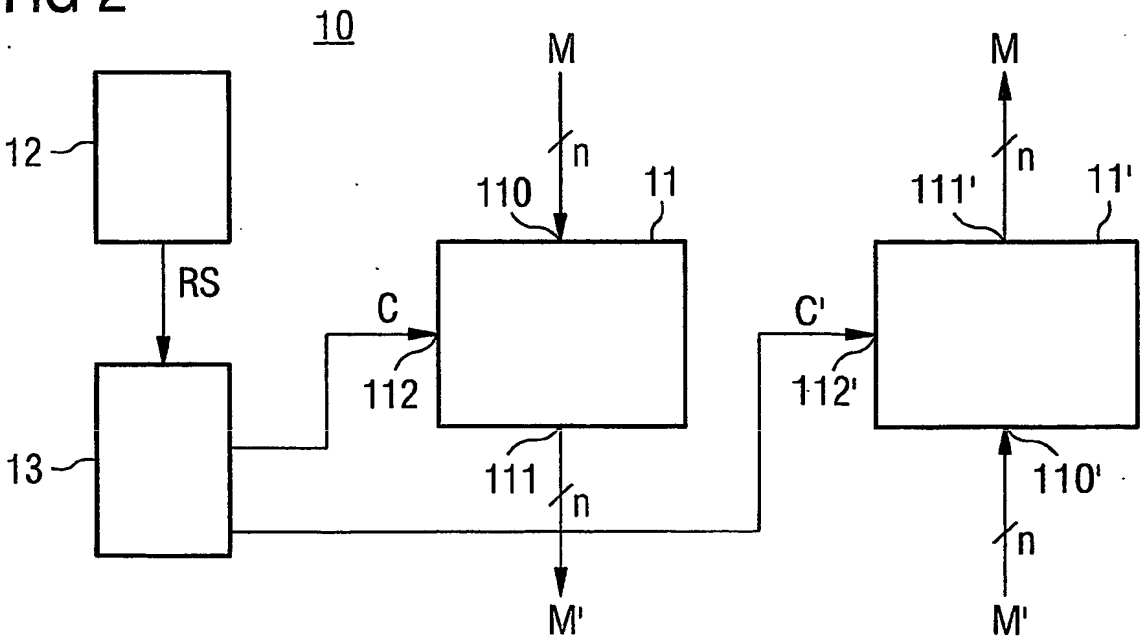

10
12
RS
13
C
112
M
n
110
11
111
n
M'
C'
112'
M
n
111'
11'
110'
n
M'

FIG 3

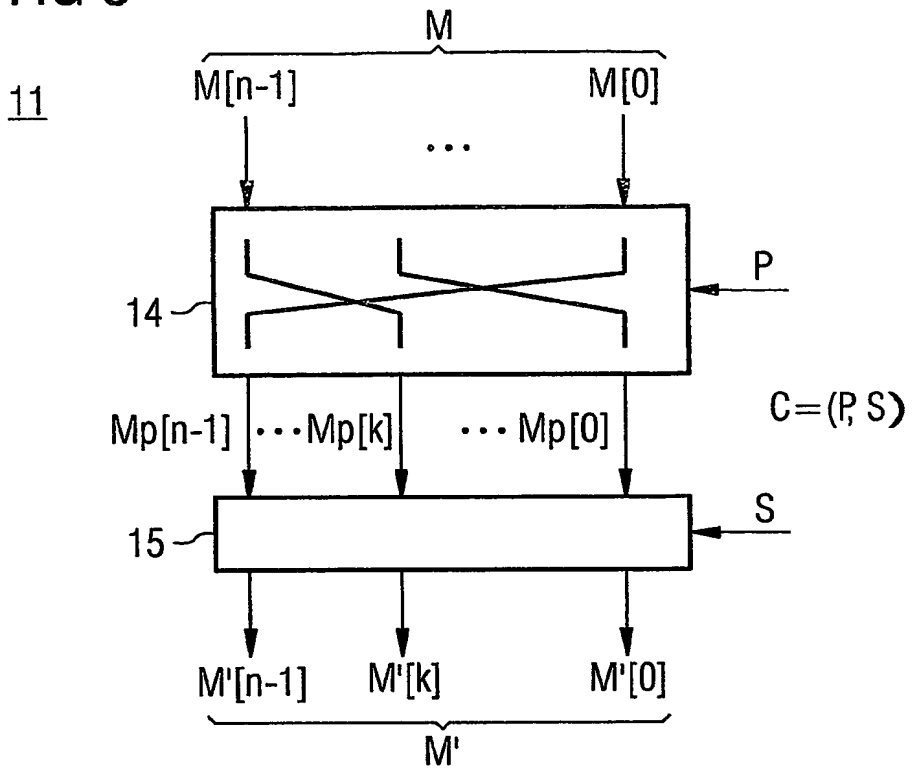

M
11
M[n-1]
M[0]
P
14
C=(P, S)
Mp[n-1]
Mp[k]
Mp[0]
S
15
M'[n-1]
M'[k]
M'[0]
M'

FIG 4

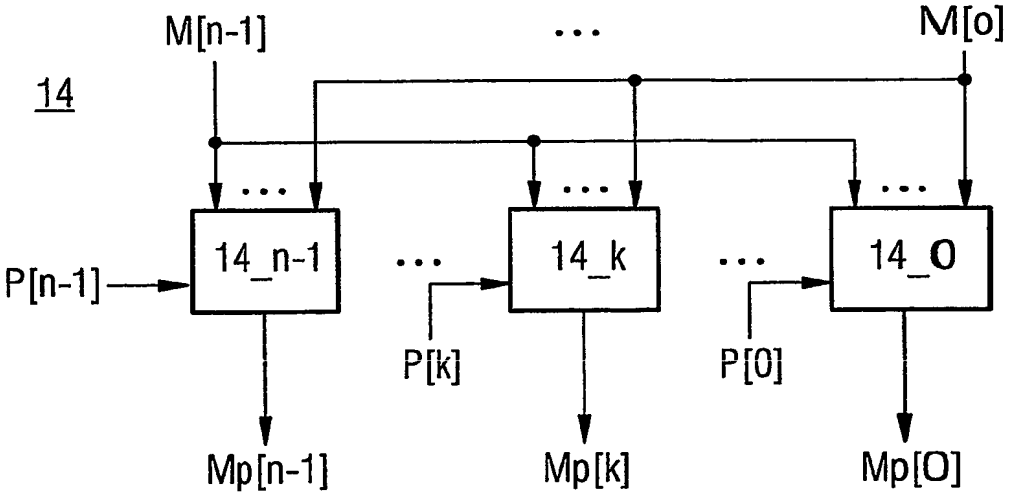

M[n-1]
M[o]
14
14_n-1
14_k
14_O
P[n-1]
P[k]
P[0]
Mp[n-1]
Mp[k]
Mp[O]

FIG 5

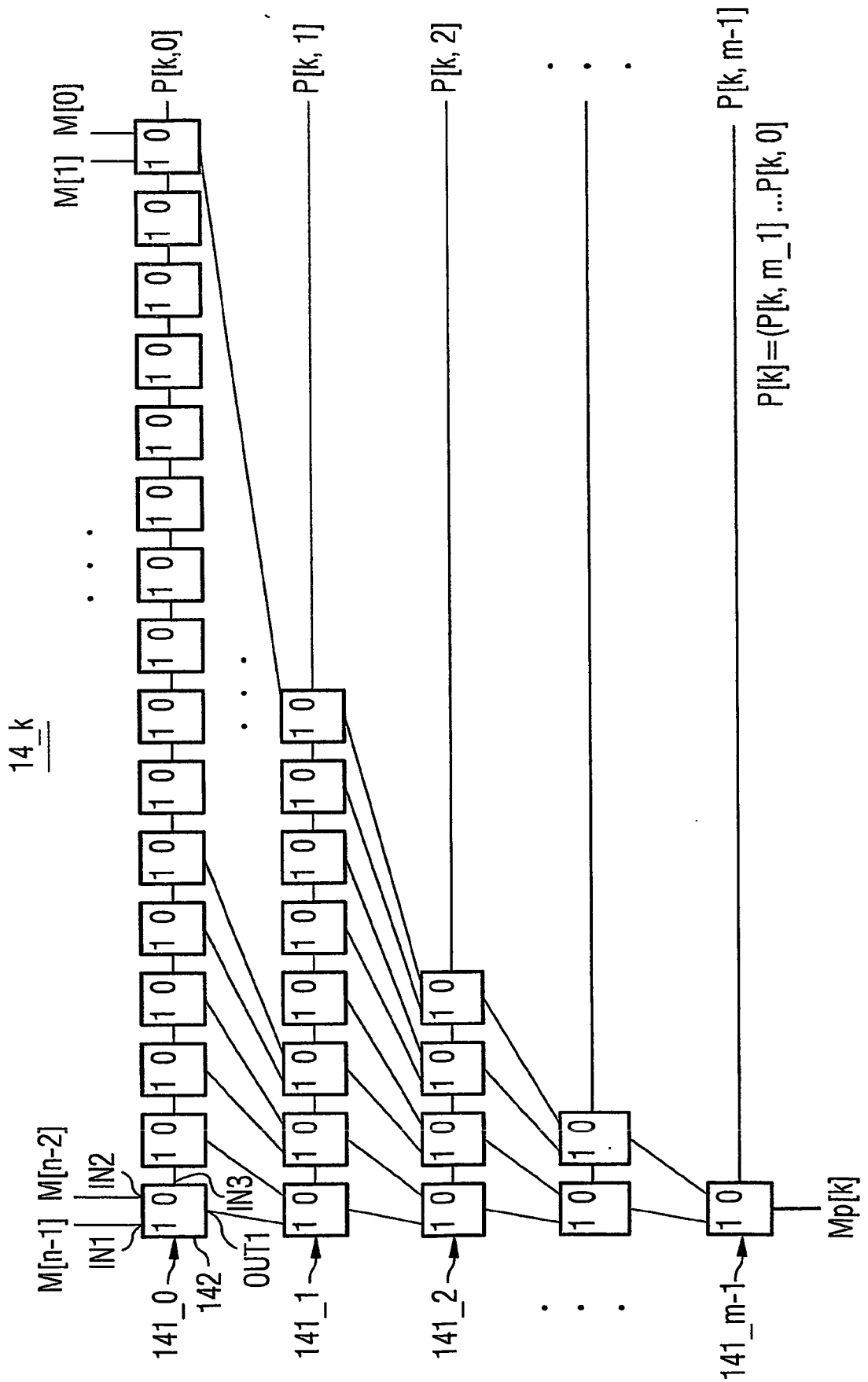

14_k
M[n-1]
M[n-2]
IN1
IN2
IN3
OUT1
142
141_0
141_1
141_2
141_m-1
M[1]
M[0]
P[k,0]
P[k, 1]
P[k, 2]
P[k, m-1]
P[k]=(P[k, m_1] ...P[k, 0]
Mp[k]
1 0

FIG 6

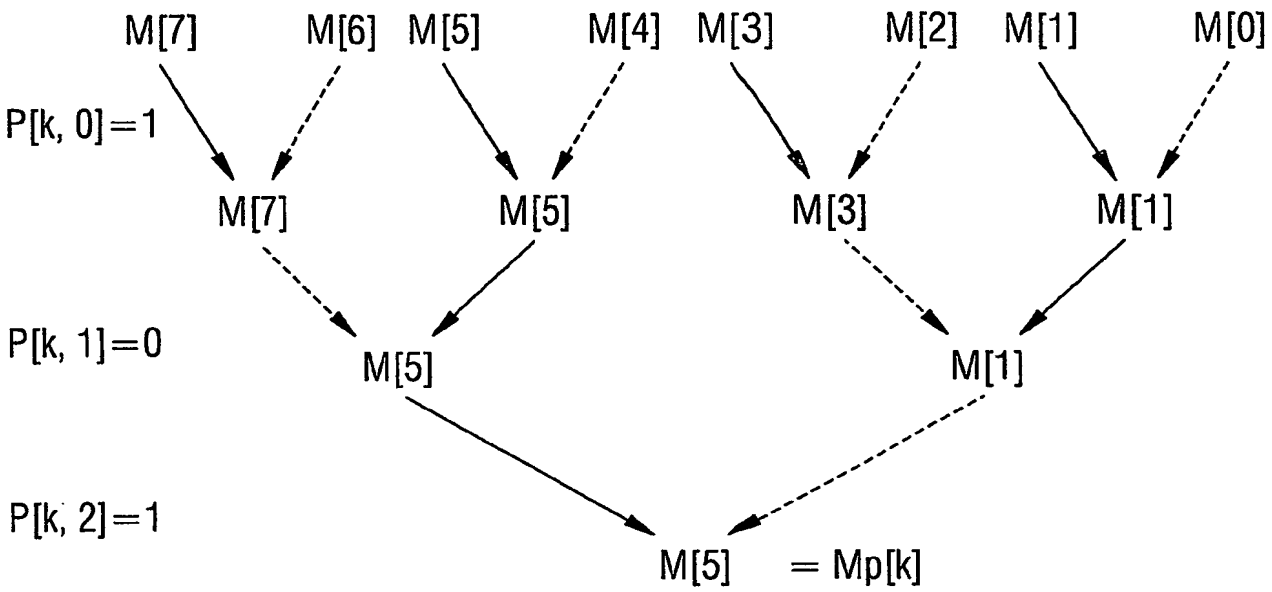


FIG 7

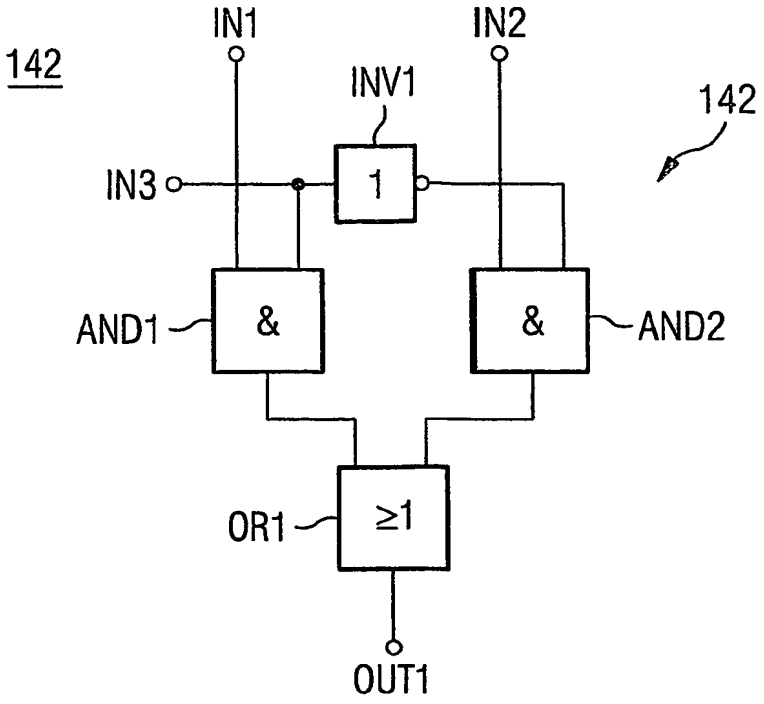
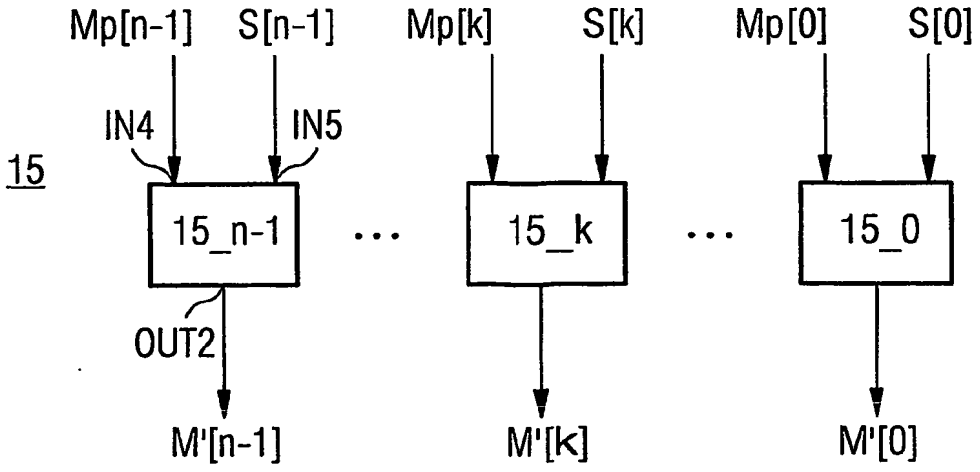


FIG 8



S=(S[n-1] ... S[0])

FIG 9

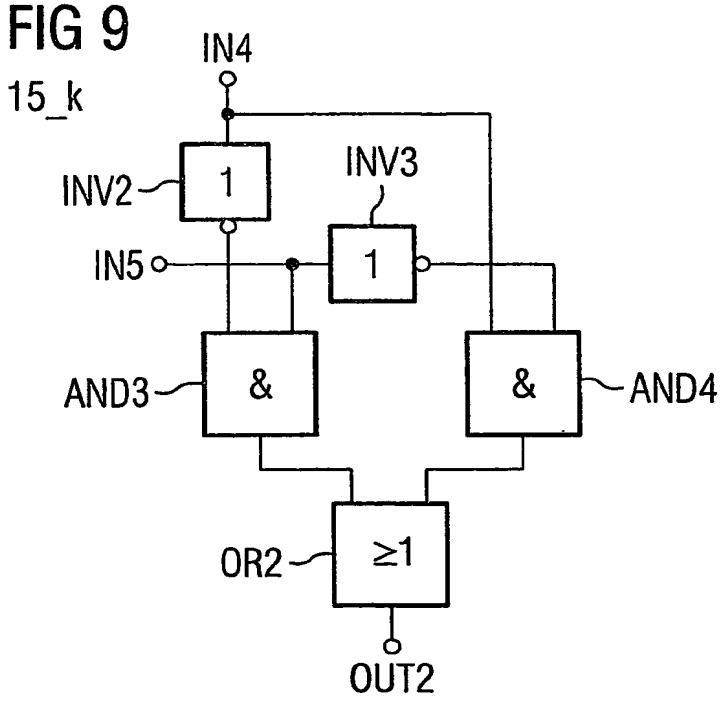


FIG 10

$$P=\underbrace{\begin{pmatrix} P[n-1, m-1] \dots P[n, 0] \\ \vdots \quad\quad \vdots \\ P[k, m-1] \dots P[k, 0] \\ \vdots \quad\quad \vdots \\ P[0, m-1] \dots P[0, 0] \\ \vdots \quad\quad \vdots \end{pmatrix}}_{n \times m} = \begin{pmatrix} P[n-1] \\ \vdots \\ P[k] \\ \vdots \\ P[0] \\ \vdots \end{pmatrix}$$

$$S=\underbrace{\begin{pmatrix} S[n-1] \\ \vdots \\ S[k] \\ \vdots \\ S[0] \\ \vdots \end{pmatrix}}_{n \times 1}$$

$$C=(P, S)$$

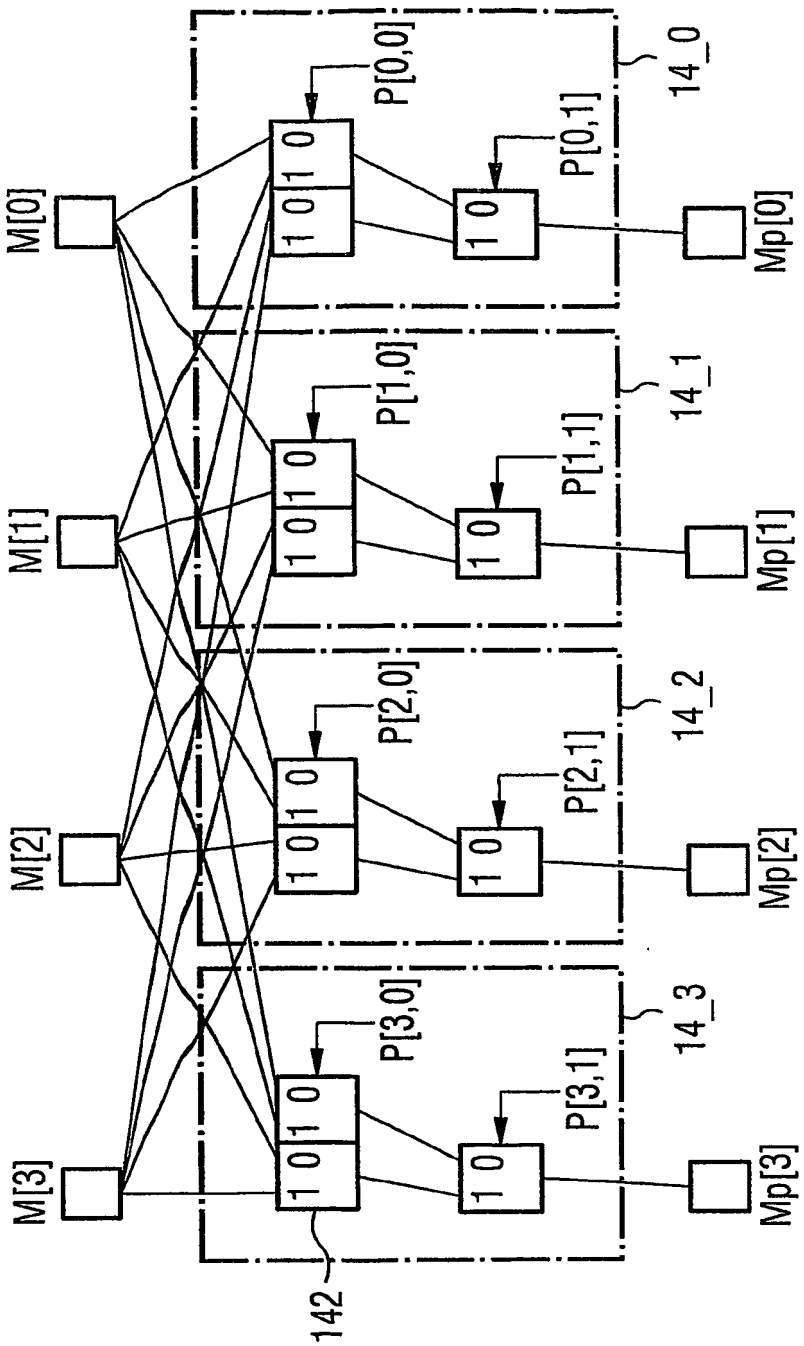

14
M[0]
M[1]
M[2]
M[3]
1 0 1 0
1 0
P[0,0]
P[0,1]
P[1,0]
P[1,1]
P[2,0]
P[2,1]
P[3,0]
P[3,1]
14_0
14_1
14_2
14_3
Mp[0]
Mp[1]
Mp[2]
Mp[3]
142

FIG 11

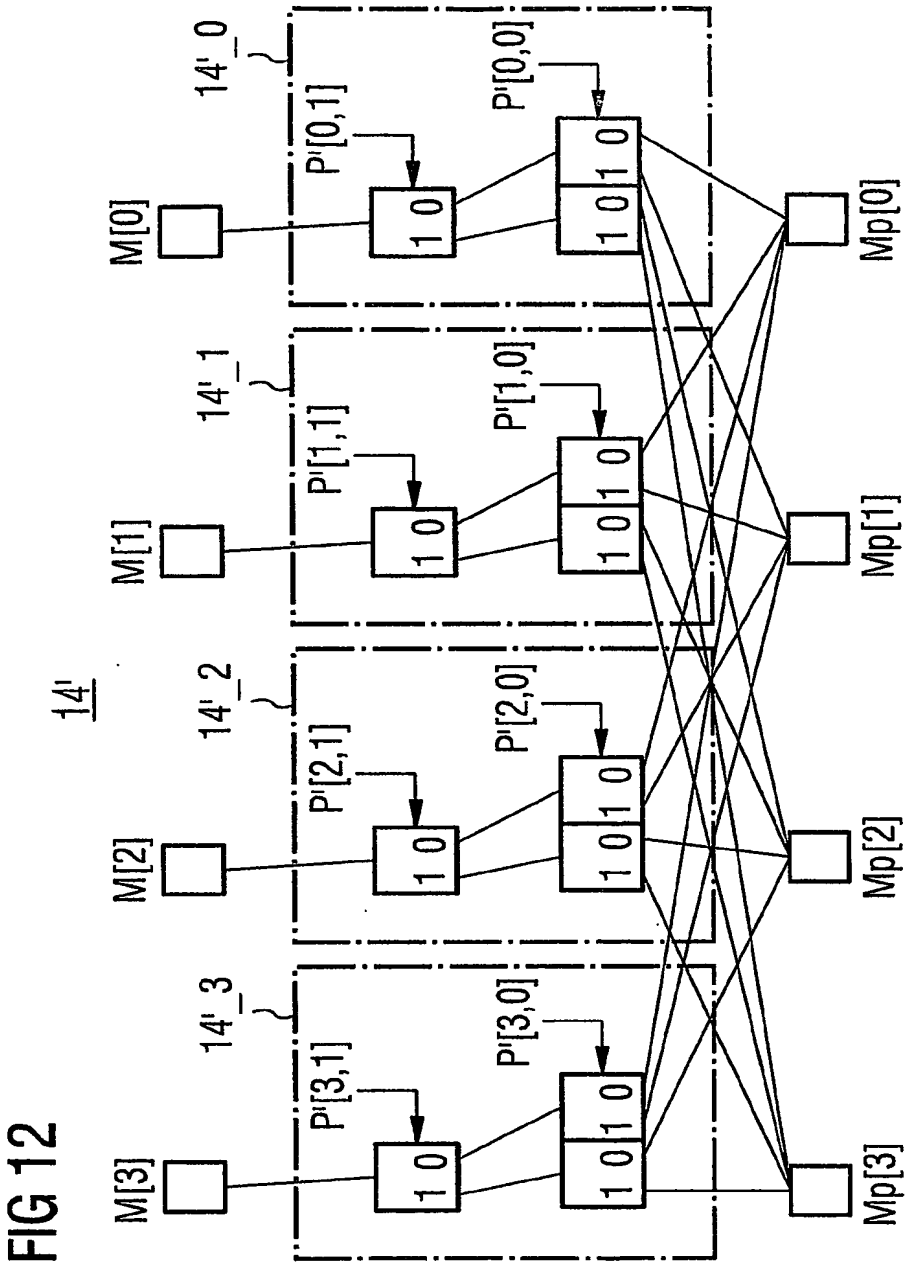
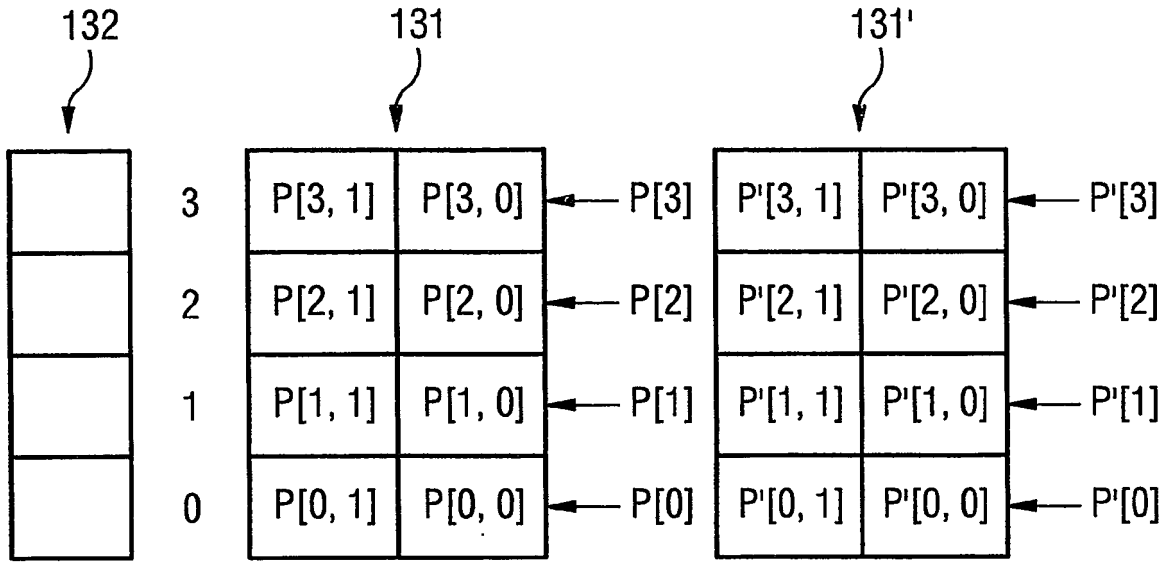

14'
14'_0
14'_1
14'_2
14'_3
M[0]
M[1]
M[2]
M[3]
P'[0,1]
P'[1,1]
P'[2,1]
P'[3,1]
P'[0,0]
P'[1,0]
P'[2,0]
P'[3,0]
1 0
Mp[0]
Mp[1]
Mp[2]
Mp[3]

FIG 12

FIG 13


132
131
131'
3
2
1
0
P[3, 1]
P[3, 0]
P[3]
P[2, 1]
P[2, 0]
P[2]
P[1, 1]
P[1, 0]
P[1]
P[0, 1]
P[0, 0]
P[0]
P'[3, 1]
P'[3, 0]
P'[3]
P'[2, 1]
P'[2, 0]
P'[2]
P'[1, 1]
P'[1, 0]
P'[1]
P'[0, 1]
P'[0, 0]
P'[0]

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/012435

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 095 525 A (ALMGREN ET AL) 10 March 1992 (1992-03-10) column 5, line 50 - column 7, line 10; figures 7a,7b	1-4,7-11
X	EP 1 022 659 A (PHILIPS INTELLECTUAL PROPERTY & STANDARDS GMBH; KONINKLIJKE PHILIPS EL) 26 July 2000 (2000-07-26) abstract; figure 2	1-4,7-11
A	"DS5002FP SECURE MICROPROCESSOR CHIP" DESCRIPTION, no. 1, February 1998 (1998-02), XP002253631 abstract	1-13
A	US 4 573 119 A (WESTHEIMER ET AL) 25 February 1986 (1986-02-25) abstract	1-13

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 February 2005	18/02/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Mezödi, S

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2004/012435

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5095525 A	10-03-1992	NONE	
EP 1022659 A	26-07-2000	DE 19901829 A1	20-07-2000
		EP 1022659 A2	26-07-2000
		JP 2000235523 A	29-08-2000
		US 6735697 B1	11-05-2004
US 4573119 A	25-02-1986	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2004/012435

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F12/14

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 095 525 A (ALMGREN ET AL) 10. März 1992 (1992-03-10) Spalte 5, Zeile 50 - Spalte 7, Zeile 10; Abbildungen 7a,7b	1-4,7-11
X	EP 1 022 659 A (PHILIPS INTELLECTUAL PROPERTY & STANDARDS GMBH; KONINKLIJKE PHILIPS EL) 26. Juli 2000 (2000-07-26) Zusammenfassung; Abbildung 2	1-4,7-11
A	"DS5002FP SECURE MICROPROCESSOR CHIP" DESCRIPTION, Nr. 1, Februar 1998 (1998-02), XP002253631 Zusammenfassung	1-13
A	US 4 573 119 A (WESTHEIMER ET AL) 25. Februar 1986 (1986-02-25) Zusammenfassung	1-13

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
1. Februar 2005	18/02/2005

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Mezödi, S

Formblatt PCT/ISA/210 (Blatt 2) (Januar 2004)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2004/012435

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
US 5095525	A	10-03-1992	KEINE		
EP 1022659	A	26-07-2000	DE	19901829 A1	20-07-2000
			EP	1022659 A2	26-07-2000
			JP	2000235523 A	29-08-2000
			US	6735697 B1	11-05-2004
US 4573119	A	25-02-1986	KEINE		